Social Media. Believe it or not, Facebook was originally conceived and implemented as a social network limited to students, especially at colleges and universities like Penn. Now, of course, millions of people around the world use it to keep up with children, grandchildren, high school classmates and other important people in their lives. And, for people in business, sports, entertainment and many other professional fields, it has become a virtual necessity to provide customers and fans a way to “follow” and “like” them. And while Facebook is undoubtedly the most widespread and popular of these networks, there are many others that target specific classes of users, such as LinkedIn and Classmates.com. A big part of the appeal and fun of these networks, of course, is to share information and updates about what’s going on in our lives, but there is an unfortunate tendency among many users to post too much personal information about themselves - birthdates (including the kids), home addresses and phone numbers and other seemingly innocuous bits of data can be gathered and assembled by people you don’t know to paint an unnervingly accurate snapshot of your life, past and present. Students leaving college for the work force have lost out on employment opportunities when prospective employers checked Facebook and found them “tagged” in photographs that seemed harmless at the time they were taken, but were deemed unprofessional after the passage of time.

Fortunately, most social networks provide at least some level of control you can use to limit who can see material you post and what information they can find out about you. Facebook, in particular, has an extensive set of controls, and they continuously refine and update them. Take the time to check out and use these controls on any social media accounts you have. On Facebook, you can do this by clicking on “Settings” (the “gear” icon) and selecting “Privacy Settings” from the menu. As with other kinds of online accounts, it’s also a good idea to periodically change your password. (See footer on next page for URL to “Top 10 Facebook Security Tips.)

The Power to “Cloud” Minds It seems like there’s a new computing “buzzword” to catch up on every week, but “cloud computing” has actually been with us for years. When network engineers draw diagrams of interconnected networks, they traditionally represent the Internet as a “cloud” to describe a place where data comes from, goes to, and resides, but exactly where and how isn’t precisely known. In usage of the past few years, “cloud computing” simply describes services and applications that are not on your personal computer or local network, but are instead “somewhere out on the Internet”. For example, most of the things Google offers, including GMail, Google Drive and Google Earth are “cloud-based”. Other examples include web-based file storage and sharing applications such as Box, virtual computing environments offered by Amazon Web Services, online file backup services such as CrashPlan,
and even Facebook can be thought of as being part of “the cloud”. And Penn actually offers a couple of “home grown” cloud services for secure file sharing and transfer, Secure Space and Secure Share.

The security consideration for Penn users who want to take advantage of “cloud” services is that much of the data they want to store, transmit and work with on these services may be sensitive, Penn-owned data that is not managed or administered by Penn. What security precautions and controls are in place to protect the data? Is strong encryption in use? What happens to the data if the company goes out of business? All these and many more questions need to be answered before you consider placing important data of any kind into the hands of a cloud service provider. Fortunately, in addition to the Penn-based services mentioned above, the University has negotiated agreements with Box (details at www.upenn.edu/computing/box) and Amazon Web Services (www.upenn.edu/computing/isc/aws). CrashPlan is also available to many Penn users. For guidance on how to evaluate the security and privacy of other third-party vendor solutions, please see www.upenn.edu/computing/security/cloud/.

Be aware, though, that some types of sensitive Penn data (e.g. patient data subject to HIPAA regulations) still may not be stored in cloud services. Check with your Local Support Provider (LSP) for more information.

Confidential/Sensitive Data What exactly is meant when a piece of data is described as “sensitive”, “confidential”, or “protected”? To answer that, think about what might happen if private data about you - your medical records, credit card numbers, Social Security number - were contained in files that were exposed due to a virus infection on your home computer. Now, broaden the scope and imagine if it wasn’t just you, but thousands of other customers at your bank, or patients at the hospital where you were recently treated. Information like this in the hands of hackers and crooks can cause embarrassment, identity theft and exposure of secrets, not to mention legal problems, unwanted publicity and loss of reputation for individuals and institutions alike.

Here at Penn there are many kinds of special data that must be protected and cared for whether your role is that of student, faculty, staff, consultant, vendor or any other affiliation (and many people wear more than one hat). Student records are subject to the Family Educational Rights and Privacy Act (FERPA), and if your work at Penn involves viewing data such as names, grades, financial aid, class lists or any other Personally Identifiable Information (PII) relating to students then you are required to take steps to protect that data. Penn departments and organizations that accept credit card payment for events such as listener fundraising drives and sporting event tickets must adhere to Federal Payment Card Industry (PCI) guidelines that mandate protection of consumer credit card data.

If you are affiliated with Penn’s Health System (UPHS), the School of Medicine, the School of Dental Medicine, the Student Health Center, the School of Nursing LIFE program, Penn’s central Human Resources department (for administration of health benefits) or any other group that deals with patient and/or health data you are almost certainly required to follow guidelines relating to Protected Health Information (PHI) under the Health Insurance
Portability and Accountability Act (HIPAA). It is important to note that HIPAA also covers participants in medical research studies conducted at Penn. If you are unsure about your HIPAA responsibilities or simply want more information about HIPAA, Penn’s Privacy Office is a good place to start (privacy@upenn.edu).

But there is a lot more than medical research going on continuously at Penn, and the world of high-stakes academic research and publication is intensively competitive. Important data falling into the hands of a rival can lead not only to lost prestige on Penn’s part, but substantial financial loss as well. If you participate in any research project at Penn, even as a student, it is vitally important that you work with your faculty and project leaders to identify and protect proprietary Penn data. In the “big picture”, no matter what sort of confidential or sensitive data you work with, any incident which results in a data breach at Penn is a potential source of financial loss, unfavorable publicity and legal liability for the University.

Of course, simply put, the best way to protect sensitive data is not to have it in the first place. It is not at all uncommon for Penn faculty and staff to have files on their personal systems that are a decade or more old, are long forgotten, or are no longer useful or needed. It is important to make sure these don’t contain sensitive data - class lists, term papers, student grades, etc. Finding this data is an important first step. Securely deleting or destroying it comes next. Your Local Support Provider (LSP) (see footer on following page) has access to tools such as Identity Finder which can locate these files, and he/she can assist you in removing them safely as well.

**Working From Home** Of course, many of us work with sensitive Penn data on a daily basis, and not only in the office but also on occasion from home or while traveling. While the data may reside on a secure server or other resource that is professionally managed and administered by highly-trained Penn IT staff, there’s a tendency for it to “leak” onto home systems, laptops, USB “thumb” drives, “smartphones” and other highly portable devices. When working from home, if at all possible, try to do your work with Penn data on a separate computer devoted to work and avoid computers that, for example, your kids use to download lots of software and files that you can’t be sure are safe. If your home computer is infected or compromised, all the data on it - including Penn’s - is at risk.

When traveling, even if it’s just down to the coffee shop at the edge of campus, use encryption tools such as PGP to protect the data on your mobile device in the event of loss or theft. If you have a laptop, consider installing LoJack (available from the Computer Connection) to remotely wipe data in the event of theft and to assist law enforcement in location and recovery. Do not store sensitive, unencrypted data on small portable (easily lost) devices such as USB “thumb” drives. If you have a Personal Data Assistant (PDA) device such as an iPhone or BlackBerry that synchronizes with a Penn server for e-mail, calendaring, backup and other functions, you must set it so that a 4-digit code is required to “unlock” it before using. Again, your LSP is a valuable source of help and guidance in this area.

Keep in mind that you must protect sensitive data not only when it’s “at rest” on your system,
you must also be sure it’s safe when you transmit it over networks. Do not send it in e-mail, either in the message body or as an attachment - e-mail is a very insecure medium. Use Secure Share and/or Secure Space to exchange sensitive, confidential files with others. Check with your LSP or visit the Penn Information Security home page at www.upenn.edu/computing/security/ for links to information about these secure file services. And for any questions you have about data and privacy, Penn’s Privacy Office is always available to help: privacy@upenn.edu.

**Disposing of Confidential and Sensitive Data** If you work with sensitive and confidential data - yours or Penn’s, and almost all of us have work and personal data on our home and work systems that we don’t want to fall into the wrong hands - you may someday need to move or delete it. Perhaps you acquire a new computer, and after transferring the data to the new system, the data likely still exists on the old system. In such instances, you’ll need to securely delete the data from the system. Note: dragging files to the “Trash” icon does not truly delete them, any more than throwing a printed document into an actual trash can “deletes” it. Retrieving files “deleted” in this way is a trivial operation.

If you own a Macintosh system, you have a “secure delete” utility built in that can be used with the “Trash” bin: drag the files into the Trash, then in the ‘Finder’ menu of the Finder application, select ‘Secure Empty Trash’. This will not only remove the files from the system, it will overwrite the space they occupied so that the contents cannot be forensically recovered. Similar applications are available for Windows (SDelete is available via download direct from Microsoft), and most Linux distributions have comparable utilities available as well.

When disposing of old hard drives, be sure the entire drive is “wiped” using a “secure delete” application before giving up possession. Even if the drive is no longer working, be aware that the drive platters can be removed, and data can be recovered from them. If your intention is that the drive is no longer to be used at all, consider destroying it entirely. There are commercial services to do this, but both the University Archives and Records Center and ISC offer this service as well. You can contact the Archives by phone at (215) 898-9432 or visit them at www.archives.upenn.edu. For ISC’s free service, visit www.upenn.edu/computing/prodesk/services/dispose.html. More information about electronic recycling at Penn can be found at www.upenn.edu/computing/provider/recycle/.

Finally, don’t forget that sensitive data printed on paper is just as sensitive as it is on a screen.
If you have confidential printouts to dispose of, don’t throw them in the trash. Shred them, or use the same services provided by the University Archives and ISC mentioned in the preceding paragraph.

*Remember, the best way to protect sensitive data is not to have it in the first place!*

**“Smartphones”, Tablets and Other Portable Devices**

If you have an iPhone, Android or other “smart” phone, take it out and look at it for a moment. The device you’re holding in your hand has vastly more computing power than the ENIAC system developed at Penn in the 1940s, not to mention the mainframes of the 1960s that filled entire rooms, and it has capabilities those old “supercomputers” could never have approached. Likewise, iPads and other “tablet” devices far outstrip the laptops of even a dozen years ago as far as bringing the world to your fingertips, no matter where in the world you are - and where the nearest electrical outlet or network port is. Early hard disks for personal computers stored only a few megabytes of data and could cost thousands of dollars. Now, you can go to your local computer “Big Box” store and buy a 64 gigabyte USB storage device for less than $50 and external drives of 2 terabytes or more for less than $200.

But of course, having portable and efficient devices like these means they are most easily lost or stolen. Theft of unattended laptops from libraries, dorm rooms, etc., continues to be among the frequently reported crimes to Penn’s Division of Public Safety. Airport waiting areas, coffee shops, book stores - especially if wireless service, free or otherwise, is offered - continue to be “happy hunting grounds” for thieves. USB drives can easily fall out of pockets while fishing for change. If you use any of these devices in conjunction with your work at Penn, there’s a very real possibility that any data on them may be exposed if stolen or lost (studies have shown that most people who find lost cell phones immediately start looking to see “what’s on it”). Most cell phones and tablets can be protected by a 4-digit “passcode” that must be entered to “unlock” the device after it has not been used after a certain length of time (and you can usually set this as well), and this a strongly recommended measure to protect important data on the device (yours and Penn’s) from compromise. For external and USB storage devices you must use encryption options such as PGP if they carry confidential or sensitive data on them. For additional suggestions, check out Top 10 Tips for Securing Your Smartphone or Tablet at www.upenn.edu/computing/security/checklists/Top10/.

**System Updates and Privileges**

Installation of regular operating system updates for desktops and laptops on a timely basis has been a standard recommendation for many years, yet many tend to overlook the fact that other portable devices we have come to rely on (e.g. smartphones and tablets) also have operating systems that must be kept current in order to provide maximum protection. Major operating systems like Windows, Mac OS X and Linux have long provided the ability to not only download and install system updates, but to do it automatically. Most phones and tablets will also alert you when updates are available. Staying up-to-date with operating system improvements is one of the most important and beneficial protections you can employ for your devices - and your data.

*“One Step Ahead” security tips: www.upenn.edu/computing/security/footprints/*
When buying a new desktop or laptop computer, especially one that is for personal use, there is an unfortunate tendency when setting up for the owner to make him- or herself an “Administrator”, “superuser”, “root”, etc. user (the description will vary by operating system). That is, a user with complete access to and control of the computer. Since you’re presumably not going to hack yourself, the thinking goes, why not set things up so you don’t have to log in as an administrative user in order to install updates, new software, etc? The problem is that a computer hacked through an administrative account gives an attacker total control of the computer and the ability to do far more damage. It’s OK - actually, pretty much necessary - to set up an administrative account for you to do important updates and installations, but for your day-to-day work it's safer to set up a “standard” or “regular” user account.

Backing Up Your Data In the Stone Age of personal computing, circa 1980, “backing up” (i.e., making copies of your files and data for safekeeping in case of system crash or other disaster) involved laboriously inserting and swapping out floppy disks by hand. For some systems, that could be more than 100 disks over the course of several hours! Some early systems such as Radio Shack’s TRS-80 even provided for backups using standard cassette tapes and recorders (also a very time- and labor-intensive process). Fortunately, backup technology has come a long way since then, as larger and larger external hard drives that can be easily used for backup purposes have become very affordable (some on the market are as large as 6 TB, or terabytes). As more and more of us do our photography, video and music in digital format, the numbers and sizes of the files we have to back up have increased exponentially, and having literally trillions of bytes of available space to make copies of them has become a necessity.

In addition to physical drives, the continuing evolution of the World Wide Web has given rise to a number of commercial online backup services such as CrashPlan and Carbonite. For a modest ongoing fee, these services will continuously scan your system for new or modified files and back them up over the web in encrypted form onto their secure servers, where you can restore them from if it becomes necessary. Some services (e.g. CrashPlan) offer plans that include unlimited space. Which of these approaches (external hard drive or online service) is better? It depends to a large degree on how valuable you feel your data is, but there is a lot of common sense in the old adage of “not keeping all your eggs in one basket”, so many people opt to do both. Modern external hard drives are highly reliable and stable, generally speaking, but they do sometimes still crash - or get stolen, are destroyed in fires, etc. The bottom line is to ask yourself, “What would happen if I lost this data - forever? How many copies do I have, and where are they?”

“Social Engineering”, “Phishing” and Identity Theft There are countless frauds, scams, hoaxes and other forms of criminal behavior floating around the Internet, and some of them, like the infamous “Nigerian Scam” have been with us for decades. Most of us have become accustomed to, if more than a bit annoyed at seeing them pop.
up in our e-mail inboxes and/or on Facebook. Sadly, the reason they continue to come around is that people still fall for them. In the U.K. in 2009, a letter carrier for the Royal Mail lost nearly $150,000 to a Nigerian operation, while in 2012 a Minnesota law firm sued Wells Fargo for not stopping payment on a $400,000 check relating to a similar swindle.

What all these frauds, etc. have in common is a phenomenon known as “social engineering”, which is another way of saying it involves a “con artist”. Social engineering can appear in the form of someone calling on the phone, claiming to be from the help desk, telling you there’s a problem with your account and that, in order to “fix” it...he needs your password. He’s relying on the fact that many if not most people will assume he’s legit and, well, give him their password. The most common, recognizable form these days is the steady drip of “phishing” e-mail messages we all receive with subject lines like “Email Quota Limit”, “Confirm Your Identity with UPenn”, “Mailbox Shutdown Notification”, “Update Your eBay Account”, etc. These messages are usually poorly written (most of them originate outside the U.S.) and claim to be from some non-existent group such as “Upenn Webmail Team” (rest assured that users at Harvard get the same messages from “Harvard Webmail Team”). Many, especially those purporting to be from major businesses of financial concerns such as eBay or PayPal will contain graphics and other features that appear absolutely authentic, probably because they’ve been pirated directly off the company’s website and other publications.

Phishing e-mails almost always include a link for you to click on and visit a website (which may also appear to be genuine, but is not) where you can enter your user name, password, account number, Social Security number, etc., to “verify” your account. Once they have this confidential information about you, the perpetrators can use it themselves or sell it to other criminals to access other online accounts of yours (people tend to use the same passwords and user names over and over), or to set up new credit accounts in your name and max them out, leaving you holding the bag. This is known as “Identity Theft”, and it continues to be a major problem in the banking and financial world. Another common form of identity theft with a more “up close and personal” touch to it is known as “skimming”. A common form of this occurs when crooks manage to affix a specially designed card reader over top of the actual card reader on an automatic teller machine (ATM) in a convenience store, travel plaza - even a bank lobby! When a customer steps up and inserts a debit or credit card, it’s read twice - once for the bank, and once for the crooks, who are close by and, in many cases, retrieving the data via a wireless connection. It’s also not uncommon for the thieves to hover around the ATM to watch the customer enter the PIN number. (Some have been known to use binoculars!) Be aware that this type of skimming is also becoming more common with gas pumps.

Skimming can also occur at places like restaurants and stores where the occasion often arises that your credit card is not always in your sight after you give it to the waiter or clerk for payment. Pocket-sized card readers can be deftly used by crooked service personnel to “skim”
your account information. Many people still hesitate to use credit cards for online purchases, but the truth is that you're probably safer using it online than in person where you can't always keep track of what's being done with your card. Few retail businesses still use credit sales slips with “carbons”, and most sales slips, restaurant slips, etc. these days will print only the last 4 digits of your account number, but it's a good practice to try to keep your credit cards in sight as much as possible.

In general, to keep yourself as safe as possible from phishing and fraudulent credit activity, here are a few basic guidelines:

- Never, ever transmit sensitive personal information in an e-mail message (very insecure)
- Never click on a link in an e-mail message from an unverified source
- Never click on any link unless you can certify where it will take you (see “Browsers”)
- Never enter sensitive personal data on a website unless you are reasonably certain the site is legitimate
- Ask for identification and verification when someone asks you to provide them with personal information about you
- Limit the amount of personal information you post on Facebook, LinkedIn, etc.
- When using ATMs and other devices with card readers, be alert to who's around, and look for any signs of tampering with the device
- When entering PIN numbers, try to position yourself so that no one else can see what you are typing
- Where possible, use ATMs, gas pumps, etc. that are in open, well-lit areas
- Check account statements as soon as they arrive, and report any discrepancies or unknown charges
- Annually check your free credit report from www.annualcreditreport.com
- Opt out of unwanted credit offers by calling (888) 5-OPT-OUT

**Physical Security** The first step in protecting yourself from computing threats in the real world is to recognize that no matter how much time you spend staring at your screen, lost in an online game or “poking” your Facebook friends, the real world never goes away! If you spend any amount of your computing time at all in an environment where there are other people around there's always the possibility that one or more of them are up to no good. “Social engineers” are adept at cruising office spaces trying to read confidential data from monitors oriented in such a way that they're more or less publicly visible. “Shoulder surfers” like to sidle up silently behind their targets and watch as they type in passwords and other sensitive data. It's not always strangers you have to watch out for - “insider” threats exist and are a danger as well. Being aware of who’s around and what they’re doing isn’t paranoid, it’s common sense.

If you are a “cubicle dweller” in your office with a standard desktop computer, it's a good idea to get into the habit of using a locking screensaver to blank your screen any time you are out of sight of your desk. If you are going to be gone for an extended time, log out of your account.
- especially if there are other people who have accounts on the same computer, and anytime you are using a “public lab” computer, such as those in Van Pelt Library.

In addition to keeping prying eyes from your monitor screen, don’t forget that sensitive, confidential information on a screen does not become less sensitive when printed out. When you’re done with sensitive printed documents, lock them up securely or shred them if they’re no longer needed. Don’t just throw them away for “dumpster divers” to retrieve.

According to Penn’s Division of Public Safety the most commonly reported crime on campus is “unattended theft”. A large chunk of these cases simply involve laptops whose owners walk away for a short time and return to find them gone. Whether in an office, library or dorm, it’s all too easy to say “I’ll only be gone a few seconds,” and end up chatting with a friend down the hall for several minutes. This is an open invitation to thieves, where using a locking screensaver won’t do you any good.

**Wireless Networking** As wireless networking (Wi-Fi, i.e., “Wireless Fidelity”) has taken hold over the past decade the number and variety of devices capable of using it has expanded far beyond laptops. “Smartphones”, iPads, Kindles, printers, home DVD players, even thermostats - all of these and more can now access the Internet (and be accessed from it) wherever they happen to be.

Penn’s commitment to provide wireless service to its ever-growing community of network users has grown to encompass not one, but two networks that now cover nearly the entire main campus. AirPennNet is a high-bandwidth, highly secure network available to anyone with an 802.1x-compliant wireless device and a PennKey (for authentication), and is able to handle the many and intensive demands placed on it by a world-class faculty, staff and student body. For those whose stay at Penn is brief and/or whose needs are not as great, AirPennNet Guest is an alternative network that is bandwidth-restricted and unencrypted, but does not require 802.1x capability (though authentication is also via PennKey). For more information on Penn’s wireless offerings (including a coverage map) visit [www.upenn.edu/computing/wireless/](http://www.upenn.edu/computing/wireless/).

But what about when you’re not at Penn? What about your own home wireless network, or the one at the coffee shop around the block, or the one in the waiting area at the airport? How do you know if it’s safe to use them? In the case of your own home network, there are steps you can take to increase security:

Need Information Security help? security@isc.upenn.edu/215-898-2172
First, be sure to select and purchase a major, reputable brand of wireless access point (WAP) for your network, especially one that offers WPA2 encryption (Wi-Fi Protected Access, Version 2 - yes, the acronyms can be confusing here), and avoid units that offer only WEP (Wireless Encryption Protocol) or, worse yet, no encryption at all. And, needless to say, configure your network (including a strong password) to use the encryption it provides.

Next, change any and all default configuration passwords to ones of your own choosing. These defaults for all manufacturers are well-known to hackers, and leaving them in place provides an “open door” to invade and take over your network.

Once you’ve done that, likewise replace the default SSID (i.e., the “network name”) supplied by the manufacturer (e.g., “linksys”) with one of your own choosing, and disable the broadcast of that SSID. This will require that authorized users of your network will need to know the SSID, and will not be able to select it from a “pull-down” menu of available known “broadcasting” networks.

Finally, if you plan to allow only a few devices to have access to your network, consider restriction by each device’s Media Access Control, or MAC address. Most WAPs will provide this option, and it’s not hard to discover the MAC address (ask your LSP to show you how if you don’t know). In fact, many devices will have it printed on the same label as the serial number.

Some “smartphones” on the market (e.g., iPhone 4 and above) provide a “personal hotspot” or other “modem” feature which allows you to turn your phone into a “mobile WAP”, and you can be generally confident in the security of this (provided you select a strong access password).

If your only option, however, is the wireless service provided by the coffee shop owner or the airport IT management, you may want to think twice, especially if it’s an “open” network (i.e., no authentication required and/or no encryption in use). You have no way of knowing whether the guy at the table next to you is really just checking his e-mail, or if he’s eavesdropping on your session and stealing your data as it’s being transmitted - especially Penn data! And if he’s not the bad guy - assuming there’s only one - it may be the woman sitting in a car in the parking lot across the street. Wireless signals don’t stop at the front door of the shop!

In short, be careful in situations where you can’t be sure who set the wireless network up or how they set it up, and avoid transmitting sensitive data over these networks whenever possible.

**Browsers** You have lots of options when it comes to using web browsers. Windows systems come with Internet Explorer (IE) installed, while Safari is supplied with Mac OS X. Most Linux systems come with browsers like Konqueror. Versions of Firefox and Chrome are available for Windows and Mac, and for some Linux versions as well. They’re all pretty much the same, right? So, which one should you use?

Actually, there is quite a wide disparity between the major browsers...
in terms of their adherence to established standards. For example, one of the buzzwords you’ll be hearing a lot in the next few years is HTML5, the latest iteration of the basic “language” of the World Wide Web. Among the browsers supported at Penn (see www.upenn.edu/computing/product/), Google’s Chrome is currently the most HTML5-compliant. On the other hand, Microsoft has been notorious over the years for engineering IE to “do its own thing”. The result is that the “look and feel” of any given web page may be noticeably different from one browser to another. In your work here at Penn, you may find that some sites do not work properly with Chrome, while some others (especially financial ones) are written to work only with IE.

The likelihood is that you may find it necessary to install and use multiple browsers on your system, and there’s nothing wrong with that - provided that you download and install updates to each of your browsers on a timely basis. Here are a few more basic tips for “safe surfing”:

- Look before you leap: when you pass your mouse cursor over a hyperlink on a page (without clicking!), check in the browser frame (usually lower left corner) to see the actual URL the link wants to take you to. If something looks odd or unusual (“Why does it say ‘hackers.org’ when this is supposed to be ‘amazon.com’?”), then think twice about clicking on the link. (And avoid clicking on links in HTML-formatted e-mail messages.)

- Don’t let browsers “remember” your passwords or “auto-complete” information on web forms: yes, it’s a convenient feature, but to “remember” all this information, the browser has to store it somewhere on your system where it may be vulnerable in the event a hacker gets in. Or, if you’re not the only person who uses the system, it may get inadvertently exposed to another user.

- Look for “secure” connections: especially when you are engaged in online financial transactions or on any site on which you need to enter sensitive information, look for “https://” (not just “http://”) in the Navigation bar (where you enter the URL) and/or look for a “padlock” icon in the browser frame that shows a “locked” state. Some browsers will also change the color of the Navigation bar when a “secure” (SSL/TLS) connection has been made. This means that your data is securely encrypted as it is transmitted.

- Block “pop-up” windows from unknown and untrusted sites: most “pop-ups” are annoying ads that, in some cases, will not go away until you completely shut down and restart your system. If you do end up with an unwanted “pop-up”, do not click on anything inside the window - close it by clicking on the “X” (Windows and most Linux varieties) or the red dot (Mac OS X) in the top corner of the frame. Many browsers will ask you if you want to accept “pop-ups” from a site before loading the page that has them, and if you’re not familiar with the site it’s a good idea to block them. Be aware, though, that some web applications you need to use (including some here at Penn) will require you to enable “pop-ups” for them.

**E-mail** Even with the rise of the World Wide Web and social networking sites like Facebook, e-mail is still the Internet feature many of us use most. It’s impossible to imagine modern
businesses and educational institutions (like Penn) being able to function without the ability to communicate with someone across campus - or on the other side of the world - in a matter of seconds.

**Spam** There’s no getting away from it, unless you want to give up using e-mail entirely. Experts estimate that as many as 4 out of 5 e-mail messages worldwide are Unsolicited Commercial E-mail (UCE), which is the official term for what we’ve all come to know as “spam”. You can’t hide from it - once you have an e-mail address it tends to get circulated around no matter how zealously you guard it, and spammers often target well-known mail hosts (like those at Penn) with messages sent to every combination of letters and digits that looks like it might be a valid account name, because there’s no cost to them if it bounces.

What’s even more galling and unnerving is when you receive a spam message that you appear to have sent to yourself, raising the possibility in your mind that your e-mail account has been “hacked”. In 99%+ of these instances, however, the answer is much simpler: for the nearly 40 years e-mail has been around, many of the headers in basic e-mail messages have been notoriously easy to forge. The “From:” header is a case in point. Spammers can just as easily make the (alleged) sender’s name “Barack Obama” as yours, and it takes a little digging into the rest of the message to see that the “Reply-to:” address is not really your own. A full discussion of e-mail headers is a bit beyond the scope of this booklet, but just be aware that there’s a lot more to an e-mail message than you usually see on your screen, and you can figure it out if you’re willing to look “under the hood”. Guess what? Your LSP can help with this, too.

Most major mail servers (including many here at Penn) have anti-spam measures in place that re-direct suspected spam messages into a separate folder (usually called “Junk”), but there will always be a few “false negatives”, i.e., spam that makes it through the filters without being flagged. Yes, it takes time, but the best thing is to simply delete them. More importantly, though, there can also be “false positives”, or legitimate messages that mistakenly get flagged as spam. A good habit to get into is to scan your “Junk” folder for these before emptying them into the trash and deleting them.

**Attachments** Exchanging files as e-mail attachments is a fast and powerful way to collaborate and get things done over great distances, or even just across campus, but there are dangers. Do you really know exactly what kind of file that is? It’s easy to disguise malware (“malicious software”) files as simple document files (PDF files especially) and fool unsuspecting recipients into opening them. Are you sure you know who the sender is? As mentioned previously, e-mail headers such as “From:” are trivially easy to forge. Do you know why the attachment was sent
to you? Did it come out of the blue, or is it something you were expecting? And, why now? This is where you need to exercise your own good judgment, but asking yourself these questions before you click to open that attachment can save you a world of headaches and heartaches. After all these years, “infected” attachments are still one of the major causes of personal computer compromises. If you are a Penn faculty or staff member who needs to exchange files securely with other Penn colleagues, consider using Penn’s new Penn+Box (www.upenn.edu/computing/box) or Secure Share (www.upenn.edu/computing/security/secure-share) services instead of e-mail to distribute files.

**Instant Messaging (IM)** Services such as Google Chat and Microsoft Messenger offer quick, efficient “real time” communication with friends, family and co-workers, but there are dangers to be aware of. Many of these services offer file transfer capabilities that permit hackers to introduce malware into a target system similar to the way e-mail attachments can. There are plenty of other ways to safely swap files, so it’s wise to avoid using IM for this purpose. In most instances, information in IM “chats” is unencrypted, and as with e-mail, care must be taken not to transmit sensitive data over IM channels. Similar to protections for social networking, be careful about how much personal information you put in your IM “profile”. And, unless you enjoy being solicited by anonymous people who troll chat services, limit your “visibility” to only those people on your “buddies” list, i.e., people you know and trust.

Users of the PennNet Phone service and those with Exchange or Zimbra accounts through Information Systems and Computing (ISC) have access to a secure, encrypted Jabber-based IM service - see www.upenn.edu/computing/im/.

**Passwords** Computer security experts around the world have been predicting the “death of passwords” for years, yet passwords are still a major part of our computing activities, and it seems like there are more of them to keep track of every day. While new authentication methods such as “tokens” will continue to supplement passwords as a way to verify identity for access to systems (“two-factor authentication”), the fact is that passwords are likely to be with us for many years to come. The advice in choosing them continues to be more or less unchanged: make them longer (8 characters minimum), complex (use uppercase, lowercase, digits and “special” characters, e.g. #, $, !), and do not base them in any way on standard dictionary words, slang phrases, etc. A good method of selection remains thinking of a phrase with special meaning only to you, taking the first letter of each word (maintaining case), and “tweaking” it with special characters. The classic example used for years (meaning, you should not use it) is “Orange elephants invade Alaska; film at eleven”, which can be worked into ‘OeiA;f@11’.

It’s a good idea to occasionally change passwords (especially your PennKey password), and it’s also suggested that you “compartmentalize” and select multiple passwords for use only with certain types of accounts. For example - and this is strongly encouraged - use your PennKey password only for PennKey-authenticated resources. Select another password for your online banking and financial accounts (including eBay and PayPal), another for online shopping, and yet another for “social media” like Facebook and LinkedIn. Even with this approach, you’re still likely to end up with a lot of username/password combinations, more than any normal person

Choose passwords with Grady the Security Dog: www.youtube.com/watch?v=jeC_KzgPNk0
can possibly hope to remember. How do you manage them all? In the last few years a large number of “password vault” applications have come on the scene. These are encrypted databases that keep track of all of your network authentication credentials. Access to them is via a strong “master password” which you select - and which, above all, is one you really need to commit to memory. While there are many commercial versions of these applications available, e.g. KeePass, your operating system may already have one. Macintosh OS X comes with an app called Keychain Access, while Windows 7 has Credential Manager.

Computers and the Law  There are many Federal and state laws that deal with crimes committed not only by criminals using computers, but crimes against computers themselves as well. Here are a few basic things you need to be aware of:

- Attacks against computers that result in financial losses, damage to medical records, physical injury to any person or any other threat to public health or safety, or damage to a system used for national defense are felony offenses.
- Accessing or attempting to access a computer with intent to defraud, or to traffic in passwords and other information for the purpose of accessing a computer without authorization is a felony offense.
- Threatening to attack or damage a computer for purposes of extortion is a felony offense.
- Monitoring and/or capturing the content of “real time” network communication (voice or data) without proper authorization is a felony offense.
- Obtaining or accessing stored electronic communications such as e-mail and voice mail without proper authorization is a felony offense.

Sadly, computers are often used to harass, intimidate, or even threaten the lives of innocent people, and at these times it becomes necessary to enlist the help of law enforcement agencies.

If you believe that any computer activity, including e-mail, is a threat to the personal safety of yourself or any other person, or represents a crime that has happened or may be about to happen, contact a law enforcement agency for investigation and guidance. At Penn, you can reach the Division of Public Safety from any campus phone by dialing 511, or from off-campus or cell phone by dialing (215) 573-3333.

“Top Ten” security lists: www.upenn.edu/computing/security/checklists/Top10/
Copyright Violation Is Illegal and Puts You and Penn at Risk

The Digital Millennium Copyright Act protects sound recordings, movies and television shows, computer games, application software, and other artistic and intellectual property that is available in electronic formats.

Copyright holders, especially in the music and entertainment industries, regularly search the Internet to find instances of illegal sharing, and college campuses like Penn are among their prime targets. Penn receives complaints alleging infringement on its networks throughout the year and is required by law to address and resolve each one. Students, faculty, staff, consultants and other Penn community members can be and have been subjected by copyright holders to lawsuits and large financial penalties. Penn does not tolerate copyright infringement by any member of the Penn Community and imposes its own sanctions:

**Students** involved in copyright infringement are subject to fines and disciplinary action by the Office of Student Conduct, including possible notation in their academic record. They may also suffer loss of network privileges and access.

**Staff** found to be engaging in infringement will receive counseling on Penn’s Acceptable Use Policy and may be subject to disciplinary action up to and including termination.

**Vendors, consultants and others** risk having their contracts terminated.

More information on U.S. Copyright Law:
http://lcweb.loc.gov/copyright/

Questions?: dmca@isc.upenn.edu

The best way to avoid having your time - and finances - disrupted by a copyright infringement action is to not engage in illegal filesharing in the first place.